UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/712,505	11/14/2000	Kevin R. Driscoll	H16-26353	9114

128 7590 11/16/2005

HONEYWELL INTERNATIONAL INC.
101 COLUMBIA ROAD
P O BOX 2245
MORRISTOWN, NJ 07962-2245

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/712,505	DRISCOLL, KEVIN R.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-43 are rejected under 35 U.S.C. 102(b) as being anticipated by Ritter(4,979,832).

3. As per claim 1, Ritter discloses a stream cipher cryptosystem(see col. 5, lines 50-52), a source for providing an encryption keystream(see col. 5, lines 50-63); an encryption combiner receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence(see col. 6, lines 8-25, 39-66) and the encryption keystream to provide a ciphertext binary data sequence(see col. 7, lines 7-12); a source for providing a decryption keystream; and a decryption combiner receiving the ciphertext binary data sequence and the decryption keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence substantially similar to the first plaintext binary data sequence(see col. 6, lines 8-25, 50-62).

4. As per claim 2, Ritter discloses the stream cipher cryptosystem wherein each operation in the second set is the inverse of an operation in the first set(see col. 6, lines 39-50, 63-68).

5. As per claim 3, Ritter discloses the stream cipher cryptosystem wherein the operations in the first set include an integer addition operation and an XOR operation, and the operations in

the second set include an integer subtraction operation and an XOR operation(see col. 10, lines 15-20, 37-48).

6. As per claim 4, Ritter discloses the stream cipher cryptosystem wherein the operations in the first set include an integer subtraction operation and an XOR operation, and the operations in the second set include an integer addition operation and an XOR operation(see col. 8, lines 39-60, col. 10, lines 15-36).

7. As per claim 5, Ritter discloses the stream cipher cryptosystem wherein the operations in the first set include a modular multiplication operation and an XOR operation, and the operations in the second set include an inverse modular multiplication operation and an XOR operation(see col. 10, lines 15-20, 37-48).

8. As per claim 6, Ritter discloses the stream cipher cryptosystem wherein the operations in the first set includes an inverse modular multiplication operation and an XOR operation, and the operations in the second set include a modular multiplication operation and an XOR operation(see col. 8, lines 39-60, col. 10, lines 15-36).

9. As per claim 7, Ritter discloses the stream cipher cryptosystem, wherein the operations in the first set include a rotate right operation and an XOR operation, and the operations in the second set include a, rotate left operation and an XOR operation(see col. 6, lines 39-50, 63-68, col. 7, lines 1-5).

10. As per claim 8, Ritter discloses the stream cipher cryptosystem wherein the operations in the first set include a rotate left operation and an XOR operation, and the operations in the second set include a rotate right operation and an XOR operation(see col. 8, lines 39-60, col. 10, lines 15-36).

11. As per claim 9, Ritter discloses a stream cipher cryptosystem(see col. 5, lines 50-52), a source for receiving a key and providing a keystream; and a cryptographic combiner receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence(see col. 6, lines 8-25, 39-66, col. 8, lines 39-60).

12. As per claim 10, Ritter discloses wherein the cryptographic combiner is an encryption combiner and the first binary data sequence is a plaintext binary data sequence and the second binary data sequence is a ciphertext binary data sequence(see col. 6, lines 39-50, 63-68).

13. As per claim 11, Ritter discloses the stream cipher cryptosystem wherein the cryptographic combiner is a decryption combiner and the first binary data sequence is a ciphertext binary data sequence and the second binary data sequence is a plaintext binary data sequence(see col. 6, lines 8-25, col. 8, lines 39-60).

14. As per claim 12, Ritter discloses stream cipher cryptosystem wherein the two sequential non-associative operations are an integer addition operation and an XOR operation(see col. 6, lines 8-25).

15. As per claim 13, Ritter discloses the stream cipher cryptosystem wherein the two sequential non-associative operations are an integer subtraction operation and an XOR operation(see col. 8, lines 14-27).

16. As per claim 14, Ritter discloses the stream cipher cryptosystem wherein the two sequential non-associative operations are a modular multiplication operation and an XOR operation(see col. 6, lines 39-50, 63-68).

17. As per claim 15, Ritter discloses the stream cipher cryptosystem wherein the two sequential non-associative operations are an inverse modular multiplication operation and an XOR operation(see col. 6, lines 8-25, col. 8, lines 39-60).

18. As per claim 16, Ritter discloses the stream cipher cryptosystem of wherein the two sequential non-associative operations are a rotate; right operation and an XOR operation(see col. 6, lines 8-25, 50-62).

19. As per claim 17, Ritter discloses the stream cipher cryptosystem of wherein the two sequential non-associative operations are a rotate left operation and an XOR operation(see col. 6, lines 39-50, 63-68).

20. As per claim 18, Ritter discloses a method of encrypting a plaintext binary data sequence, the method generating an encryption keystream as a function of a key(see col. 6, lines 8-25); and combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence(see col. 7, lines 7-40).

21. As per claim 19, Ritter discloses wherein the two non-associative operations include an integer addition operation(see col. 8, lines 30-65).

22. As per claim 20, Ritter discloses the wherein the two non-associative operations include an XOR operation(see col. 8, lines 19-27).

23. As per claim 21, Ritter discloses wherein the two non-associative operations include an integer subtraction operation(see col. 6, lines 25-50).

24. As per claim 22, Ritter discloses wherein the two non-associative operations include an XOR operation(see col. 6, lines 39-50, 63-68).

25. As per claim 23, Ritter discloses wherein the two non-associative operations include a

modular multiplication operation(see col. 8, lines 39-60, col. 10, lines 15-36).

26. As per claim 24, Ritter discloses wherein the two non-associative operations include an XOR operation(see col. 6, lines 39-50, 63-68).

27. As per claim 25, Ritter discloses wherein the two non-associative operations include an inverse modular multiplication operation(see col. 6, lines 39-50, 63-68).

28. As per claim 26, Ritter discloses wherein the two non-associative operations include an XOR operation(see col. 8, lines 30-65).

29. As per claim 27, Ritter discloses wherein the two non-associative operations include a rotate right operation(see col. 6, lines 8-25, 50-62).

30. As per claims 28, 30, limitations already addressed(see claim 24).

31. As per claim 31, limitations have already been addressed(see claim 1).

32. As per claim 32, wherein the two non-associative operations include an integer addition operation(see col. 8, lines 30-65).

33. As per claim 33, already rejected(see claim 24).

34. As per claim 34, already rejected(see claim 21).

35. As per claims 35, 37, 39, limitations already rejected(see claim 24).

36. As per claim 36, limitations already rejected(see claim 23).

37. As per claim 38, limitations already rejected(see claim 25).

38. As per claims 39, 43, limitations already rejected(see claim 24).

39. As per claim 40, limitations already rejected(see claim 27).

40. As per claims 41, 43, limitations already rejected(see claim 24).

41. As per claim 42, limitations already rejected(see claim 7).

Response to Amendment

42. The Applicant states that Ritter does not teach or suggest combining a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence. The Examiner disagrees with the Applicant. Ritter discloses a ciphering system that includes enciphering and deciphering (see col. 5, lines 50-54). The combiner of Ritter discloses a substitution combiner and inverse of substitution (see col. 6, lines 8-25). Ritter discloses that exchanges two substitution elements; these elements are selected by the plaintext value and the pseudo-random value. The plaintext input is enciphered and then deciphered as the extractor output(see col. 7, lines 29-55). The Applicant states that Ritter teaches away from exclusive or system. The Examiner disagrees with the Applicant. Ritter teaches an improvement upon exclusive or(see col. 3, lines 23-62).

43. The Applicant states that the two sequential non-associative operations according to claims 1, 9, 18, and 31 can be implemented with XOR. However, in claims 1, 9, 18, and 31 XOR is not claimed. The claims call for two non-associative operations. Ritter discloses a substitution combiner and inverse of substitution (see col. 6, lines 8-25). If the Applicant wishes to define and claim in the independent claims more specifically which two non-associative operations are being used, the Applicant is urged to do so. Otherwise, the claims are interpreted broadly in light of the specification.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

November 10, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100